文章编号:1674-7070(2010)01-0088-04

网络入侵检测与漏洞扫描协作研究

刘秀玲[1]　詹仕华[1]

摘要

入侵检测系统是现今网络信息安全研究的热点,普通的网络入侵检测系统有较高的误报率,为了减少误报率并提高检测效率,首先在入侵检测系统的分析引擎中采用将异常检测和误用检测结合起来降低入侵检测系统的误报率和漏报率,然后再通过漏洞扫描引擎过滤入侵检测系统中无效警报再次降低误报率,最后通过响应界面报警.

关键词

入侵检测系统;误报率;漏洞扫描;协作

中图分类号 TP393

文献标志码 A

0　引言
Introduction

入侵检测系统(Intrusion Detection System,IDS)采用的是一种积极主动的安全防护技术,可以识别出系统是否被入侵,从而做出及时的反应.一般来说,传统的模式匹配方法是将数据包中内容与系统已知入侵特征库中的攻击特征串机械地进行匹配,只要发现数据包中的内容与攻击特征相匹配,就马上发出警报,并不判断它是不是真的攻击行为,这样就不可避免地产生误报[1-2].例如当攻击利用的 Microsoft IIS 上的一个漏洞,而目标系统上运行的是 Linux + Apache,在这种情况下所产生的报警就是误报,实际上该入侵是不能成功的.通过漏洞扫描可以有效降低 IDS 误报率,提高 IDS 效率.

1　入侵检测与漏洞扫描
Intrusion detection and vulnerability scanning

1.1　入侵检测

入侵检测是一种对系统的运行状态进行监视,发现各种攻击企图、攻击行为或攻击结果,以保证系统资源的机密性、完整性与可用性的技术.它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象,是一种主动防御技术.

从数据来源分类,入侵检测系统分为基于网络的入侵检测系统、基于主机的入侵检测系统、分布式入侵检测系统 3 种.

1.2　网络漏洞扫描

网络漏洞扫描器通过远程检测目标主机 TCP/IP 不同端口的服务,记录目标给予的应答,来搜集目标主机上的各种信息,然后与系统的漏洞库进行匹配,如果满足匹配条件,则认为安全漏洞存在;或者通过模拟黑客的攻击手法对目标主机进行攻击,如果模拟攻击成功,则认为漏洞存在.

2　入侵检测与漏洞扫描协作设计
The design of intrusion detection collaborating with vulnerability scanning

2.1　总体结构

基于网络的入侵检测引擎将检测到的入侵先记入到漏洞扫描引

收稿日期 2009-10-31

资助项目 福建省教育厅项目(JB06119);福建农林大学青年基金(07B21)

作者简介

刘秀玲,女,硕士,讲师,主要从事通信及数据库研究. liuxiuling50@163.com

1　福建农林大学　计算机与信息学院,福州,350002

擎中,经过漏洞扫描引擎降低误报率后再通过响应界面报警,漏洞扫描引擎中的过滤结果可以及时更新入侵检测引擎中的入侵规则. 其总体结构设计如图 1 所示.

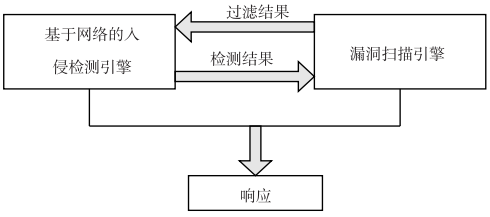

图 1 系统结构

Fig. 1 System framework

2.2 基于网络的入侵检测引擎

基于网络的入侵检测引擎由探测器、数据预处理、分析引擎、网络安全数据库等几部分组成,其结构如图 2 所示.

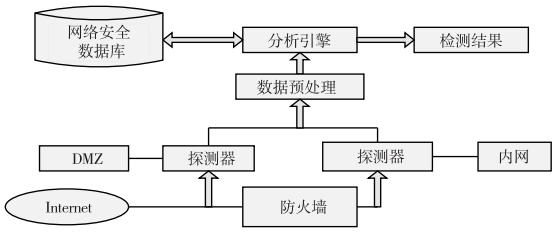

图 2 基于网络的入侵检测引擎结构

Fig. 2 Engine structure of network-based intrusion detection

2.2.1 探测器

对于基于网络的入侵检测系统,数据主要来源于网络通信数据流. 各种探测器放在不同位置截获网络上的数据包,并确保能够准确捕获所必需数据,例如 IP 和 TCP 报头等. 网络适配器常用的 2 种接收模式是普通模式和混杂模式,在普通模式下,网络适配器只接收属于自己的数据包;在混杂模式下,网络上所有的数据包都会被接收. 通过将网络适配器设置为混杂模式,来达到监听并采集网段上的所有传输数据包的目标. 在 Linux,Solaris 等系统平台下可以采用 LibPCap(Packet Capture Library)开发包来采集数据. LibPCap 是专门为数据监听应用程序设计的开发包,用于访问数据链路层数据. 该库提供的 C 函数接口可以捕获经过网络接口的数据包. 如果是基于 Win32 平台的可以采用 WinPCap 开发包,该开发包基于 LibPCap 函数库和 BPF 模型,是 LibPCap 在 Win32 平台上的移植,可以进行网络数据包的捕获、分析和发送.

2.2.2 数据预处理

数据预处理就是对数据包进行格式转换形成标准记录格式,以方便分析引擎对数据包的检查和处理. 数据预处理模块实现模拟 TCP/IP 协议栈功能,如 IP 碎片重组、TCP 流重组与 Http,Unicode、RPC 和 Telnet 解码等功能[3].

2.2.3 分析引擎

基于统计分析原理的异常检测能够检测未知的入侵行为,漏报率低;但当用户众多、用户行为经常改变时误报率高. 基于模式匹配原理的误用检测技术成熟,误报率低;但不能检测到未知的入侵行为,漏报率高. 因此入侵检测系统要将误用检测与异常检测结合起来,互相弥补彼此的不足,降低误报率与漏报率,分析引擎结构如图 3 所示.

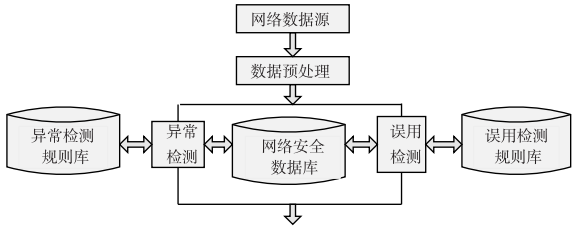

图 3 分析引擎结构

Fig. 3 Structure of analysis engine

2.2.4 网络安全数据库

网络安全数据库存放系统的历史数据和检测的中间结果等,是不同部件之间数据处理的共享数据库,为系统不用部件提供各自感兴趣的数据,因此应该提供灵活的数据维护、处理和查询服务.

2.3 漏洞扫描引擎

漏洞扫描引擎[4]一般由警报数据库、漏洞扫描器、漏洞分析器、漏洞数据库、警报过滤引擎组成,其结构如图 4 所示.

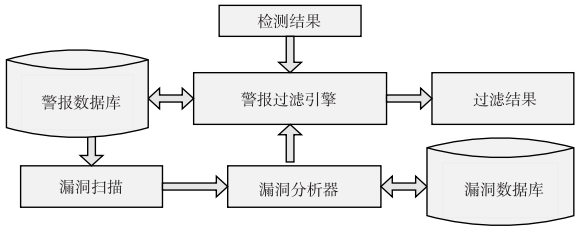

图 4 漏洞扫描引擎结构

Fig. 4 Engine structure of vulnerability scanneing

2.3.1 警报数据库

警报过滤引擎将入侵检测引擎发送来的检测结果先进行冗余警报消除处理,然后录入到警报数据库中,以免因入侵检测引擎对一次持续性攻击产生多个入侵事件的报告.

2.3.2 漏洞扫描

通过使用漏洞扫描器可以发现网络和主机存在的对外开放的端口、提供的服务、某些系统信息、错误的配置等,包括服务类型、源目的地址、源目的端口、报文长度、连接建立时间、连接持续时间,报文的大小等信息,每一个连接对应一个记录. 例如一个TCP 连接建立的时间、连接持续的时间、建立连接双方的主机 IP 地址及端口、两个方向的流量、连接的结束状态等.

2.3.3 漏洞分析器

漏洞分析器的主要功能是发现系统的安全漏洞. 漏洞分析器将漏洞扫描器收集到的数据与漏洞库中的漏洞信息进行对比分析,根据匹配结果发现漏洞.

2.3.4 漏洞数据库

漏洞数据库中记载网络中相关漏洞信息,漏洞的命名采用 CVE 标准,以便于漏洞数据库的及时更新以及漏洞扫描与入侵检测系统的信息交换. 由于新的漏洞会不断出现,该数据库需要经常更新,以便能够检测到新发现的漏洞.

2.3.5 警报过滤引擎

警报过滤引擎将引发本警报的攻击所对应的漏洞信息提取出来并在漏洞数据库中查找,看被攻击网络上是否存在这个漏洞,若存在则通过响应接口报警,若不存在则该警报无效,只是将警报信息记入日志中. 若被攻击网络上是否存在此漏洞尚未确定,也就是漏洞扫描器尚未对网络上的相应漏洞进行扫描,这时向响应界面发出警报,并提示攻击成功与否尚未验证,同时向漏洞扫描器提交扫描请求,对相应漏洞进行扫描,并将扫描结果写入漏洞数据库中.

2.4 响应

响应界面向管理员提供管理和监控系统运行的模块,通过该模块,管理员可以对整个系统进行报警信息查看、管理,以及系统维护、各种参数和阈值设定等工作. 当检测到入侵发生时,响应系统记录入侵时间,以屏幕显示、发电子邮件和手机短信息等形式通知管理人员攻击成功的可能性以及严重程度并做出相应响应. 严重的入侵可以切断网络连接,截断攻击者和目标主机之间的连接,避免系统受到进一步的侵害.

2.5 通信服务

网络入侵检测引擎和漏洞扫描引擎之间的通信服务是非常重要的,是两者之间传送信息的桥梁. 通信服务能够保证将网络入侵检测引擎的检测结果传送给漏洞扫描引擎,并将漏洞扫描引擎的过滤结果反馈给网络入侵检测引擎. 通信服务主要记录网络入侵检测引擎与漏洞扫描引擎之间的通信方式,可以为数据包提供路由服务,它的主要任务是数据包的接收和转发[5]. 为保护通信信息的机密性和完整性,网络入侵检测引擎和漏洞扫描引擎之间在进行通信之前应该经过授权和认证,确认通讯双方的合法性;同时它们之间的通信应该进行加密.

3 设计模型优点

Advantages of the designed model

1) 误报率低. IDS 一旦检测到入侵并不会马上发出报警,而是先通过漏洞扫描引擎判断是否是真的入侵,根据过滤结果的反馈,抛弃不能成功的入侵,尽可能地减少误报率,提高报警率.

2) 检测效率高. IDS 可以根据扫描结果将模式库中与该漏洞相关的攻击模式删除,从而极大地减少模式匹配的数量,提高检测速度.

3) 抗攻击性强. 网络入侵检测通过与漏洞扫描协作,及时修补系统漏洞,从而增强了系统的抗攻击性.

4) 规则库动态更新. IDS 根据漏洞扫描结果及时删除已得到修补的漏洞的入侵模式,减小规则库的规模;并且规则库自动更新新发现的安全漏洞.

基于网络的入侵检测系统引擎根据漏洞扫描引擎过滤的结果,将分析引擎规则库中已得到修补的安全漏洞相关的攻击特征删除,以减少规则库中攻击模式的数量. 通过漏洞扫描与入侵检测系统的协作,可以有效地提高 IDS 检测效率,增强系统的整体防御能力.

参考文献

References

[1] 黄烟波,汪建波,王科. 入侵检测系统中误报与漏报现象研究[J]. 中国科技信息,2006(20):156-157
HUANG Yanbo, WANG Jianbo, WANG Ke. Research on false alarm and missed alarm of intrusion detection system[J]. China Science and Technology Information, 2006(20):156-157

[2] 向碧群,黄仁. 漏洞扫描技术及其在入侵检测系统中的应用

[J]. 计算机工程与设计,2006,27(7):1301-1304
XIANG Biqun, HUANG Ren. Vulnerability-scanning technology and its application in intrusion detection system[J]. Computer Engineering and Design,2006,27(7):1301-1304
[3] 景志刚. 基于网络的入侵检测系统的研究和实现[D]. 郑州:郑州大学信息工程学院,2005
JING Zhigang. Research on and implementation of network-based intrusion detection system[D]. Zhengzhou:Zhengzhou University College of Information Engineering,2005
[4] 张涛,郝红卫. 基于安全扫描信息降低入侵检测系统的误报率[J]. 微计算机信息,2006,22(8-3):61-63
ZHANG Tao,HAO Hongwei. Reducing the false rate of intrusion detection system based on security scanning information[J]. Microcomputer Information,2006,22(8-3):61-63
[5] 段丹青,陈松乔,杨卫平. 融合漏洞扫描的入侵检测系统模型的研究[J]. 计算机技术与发展,2006,16(5):131-133,142
DUAN Danqing,CHEN Songqiao,YANG Weiping. Study of an intrusion detection system model merged with vulnerability scanner[J]. Computer Technology and Development,2006,16(5):131-133,142

Research on collaboration between network intrusion detection and vulnerability scanning

LIU Xiuling[1] ZHAN Shihua[1]
1 College of Computer & Information,Fujian Agriculture and Forest University,Fuzhou 350002

Abstract Nowadays intrusion detection system is a focus in research on network information security,but network intrusion detection system has a high false alarm rate. In order to reduce the false alarm rate of network intrusion detection system and improve detection efficiency,anomaly detection and misuse detection were first combined in analysis engine of intrusion detection system to reduce the false alarm rate and omission rate,then filtered invalid alerts through vulnerability scanner to reduce false alarm rate again,and finally gave a warning by the response interface.
Key words intrusion detection system;false alarm rate;vulnerability scanning;collaboration